



Storage Area Network (SAN) Checklist for Sharing Peripherals Across the Network Security Technical Implementation Guide Version 1 Release 1

06 Janauary 2006

Developed by DISA for the DOD

Database Reference Number:		CAT I:
Database entered by:	Date:	CAT II:
Technical Q/A by:	Date:	CAT III:
Final Q/A by:	Date:	CAT IV:
		Total:

FOUO UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist Confidential System = CONFIDENTIAL Checklist Secret System = SECRET Checklist Top Secret System = SECRET Checklist

Enclave R	eviewer				Phone				
Previous S	RR	Y	N	Date of Previous SRR		S01 A	vailable	Y	N
Number of	f Current ()pen F	inding	s					
Site									
Name									
Address									
Phone									

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

SAN03.001.00	CAT: 1	Zoning is not used to protect the SAN.
8500.2 IA Control:	ECCD-1: ECCD-2	Category: 2.1 - Object Permissions
Condition(s):	SANS Storage Device	ce: SANS Switch
Target(s):	SANS Storage Device	ce; SANS Switch
Vulnerability	Zoning is not used to	protect the SAN
	result, storage resour	t method of managing, partitioning, and controlling pathways to and from storage devices on the SAN fabric; as a arces are maximized, and data integrity and data security are maintained. Insure that zoning is used to protect the SAN.
References:	SHARING PERIPHEI	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:	SPAN SAN03.001.00	0: The reviewer with the assistance of the IAO/NSO, verify that zoning is used to protect the SAN
Fix(es):	plan and then, followi	0: Develop a zone topography, from the topography create a plan to implement zoning, obtain CM approval of the ving the plan, reconfigure the SAN to support zoning.
OPE	N: NOT	Γ A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		
SAN03.002.00	CAT: 2	Hard zoning is not used to protect the SAN.
8500.2 IA Control:	ECCD-1: ECCD-2	Category: 2.1 - Object Permissions
Condition(s):	SANS Storage Device	ce: SANS Switch
Target(s):	SANS Storage Device	ce; SANS Switch
Vulnerability	Hard zoning is not us	sed to protect the SAN.
	controlled by software	osed to soft zoning, is enforced by the port hardware level and is harder to subvert than soft zoning which is re. sure that hard zoning is used to protect the SAN.
References:	SHARING PERIPHEI	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:	SPAN SAN03.002.00	0: The reviewer, with the assistance of the IAO/NSO, will verify that hard zoning is used to protect the SAN.
Fix(es):		0: If zoning has not been implemented, develop a zone topography, from the topography create a plan to ng, obtain CM approval of the plan and then, following the plan, reconfigure the SAN to support hard zoning.
		implemented develop a plan to migrate to hard zoning, obtain CM approval of the plan and then, following the plan, to support hard zoning.
ОРЕ	N: NOT	Γ A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		

SAN03.003.00	CAT: 2 The	default zone visibility is not set t	to "none"
8500.2 IA Control:	ECCD-1: ECCD-2	Category: 2.1 - Object Per	rmissions
Condition(s):	SANS Switch: SANS Storage	Device	
Target(s):	SANS Storage Device; SAN	S Switch	
Vulnerability	The default zone visibility sett	ting is not set to "none".	
	are not explicitly placed into.	tting is set to "none", new clients brought into the SAN t the default zone visibility setting, if available, is set to	•
References:	SHARING PERIPHERALS AG	CROSS THE NETWORK SECURITY TECHNICAL IM	MPLEMENTATION GUIDE
Checks:	SPAN SAN03.003.00: Reviet this setting is not available ma	wer with the assistance of the IAO/NSO, verify that the ark this check as N/A.	ne default zone visibility setting is set to "none" If
Fix(es):	into the correct zone(s) and a	e all clients that have not been explicitly placed into a fter doing so the plan will include the modification of the following the plan, reconfigure the SAN to allow for the second of the second of the second of the sec	the default zone visibility setting to "none". Obtain CM
ОРЕ	N: NOT A FI	NDING: NOT REVIEWED:	NOT APPLICABLE:
Notes:			
Notes:			
Notes: SAN03.004.00	CAT: 3 Har	d zoning, using Port World Wide	Names (PWWN)
		d zoning, using Port World Wide Category: 2.1 - Object Per	,
SAN03.004.00 8500.2 IA Control:		Category: 2.1 - Object Per	,
SAN03.004.00 8500.2 IA Control: Condition(s):	ECCD-1: ECCD-2	Category: 2.1 - Object Per	,
SAN03.004.00 8500.2 IA Control: Condition(s): Target(s):	ECCD-1: ECCD-2 SANS Storage Device: SANS SANS Storage Device; SAN	Category: 2.1 - Object Per	rmissions
SAN03.004.00 8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	ECCD-1: ECCD-2 SANS Storage Device: SANS SANS Storage Device; SAN Hard zoning, using Port World Hard zoning, as apposed to s controlled by software.	Category: 2.1 - Object Per S Switch S Switch d Wide Names (PWWN), is not used to protect the SA oft zoning, is enforced by the port hardware level and	AN. I is harder to subvert than soft zoning which is
SAN03.004.00 8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	ECCD-1: ECCD-2 SANS Storage Device: SANS SANS Storage Device; SAN Hard zoning, using Port World Hard zoning, as apposed to s controlled by software. The IAO/NSO will ensure that	Category: 2.1 - Object Per S Switch S Switch d Wide Names (PWWN), is not used to protect the SA	AN. d is harder to subvert than soft zoning which is l), is used to protect the SAN.
SAN03.004.00 8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	ECCD-1: ECCD-2 SANS Storage Device: SANS SANS Storage Device; SAN Hard zoning, using Port World Hard zoning, as apposed to s controlled by software. The IAO/NSO will ensure that SHARING PERIPHERALS AG	Category: 2.1 - Object Per S Switch S Switch d Wide Names (PWWN), is not used to protect the SA oft zoning, is enforced by the port hardware level and thard zoning, using Port World Wide Names (PWWN) CROSS THE NETWORK SECURITY TECHNICAL IM eviewer with the assistance of the IAO/NSO, verify tha	AN. It is harder to subvert than soft zoning which is I), is used to protect the SAN. IPLEMENTATION GUIDE
SAN03.004.00 8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	ECCD-1: ECCD-2 SANS Storage Device: SANS SANS Storage Device; SAN Hard zoning, using Port World Hard zoning, as apposed to s controlled by software. The IAO/NSO will ensure that SHARING PERIPHERALS AG SPAN SAN03.004.00: The re (PWWN), is used to protect the	Category: 2.1 - Object Per S Switch S Switch d Wide Names (PWWN), is not used to protect the SA oft zoning, is enforced by the port hardware level and thard zoning, using Port World Wide Names (PWWN) CROSS THE NETWORK SECURITY TECHNICAL IM eviewer with the assistance of the IAO/NSO, verify tha	AN. d is harder to subvert than soft zoning which is l), is used to protect the SAN. MPLEMENTATION GUIDE at hard zoning, using Port World Wide Names
SAN03.004.00 8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	ECCD-1: ECCD-2 SANS Storage Device: SANS SANS Storage Device; SAN Hard zoning, using Port World Hard zoning, as apposed to s controlled by software. The IAO/NSO will ensure that SHARING PERIPHERALS AG SPAN SAN03.004.00: The re (PWWN), is used to protect the SPAN SAN03.004.00: Development	Category: 2.1 - Object Per S Switch S Switch d Wide Names (PWWN), is not used to protect the SA oft zoning, is enforced by the port hardware level and thard zoning, using Port World Wide Names (PWWN) CROSS THE NETWORK SECURITY TECHNICAL IM eviewer with the assistance of the IAO/NSO, verify that he SAN. op a plan to migrate the SAN to Hard Zoning, obtain Carrell 1985.	AN. d is harder to subvert than soft zoning which is l), is used to protect the SAN. MPLEMENTATION GUIDE at hard zoning, using Port World Wide Names

SAN03.005.00	CAT: 1	The zoning tables on all affected HBAs reset
8500.2 IA Control:	DCSS-1: DCSS-2	Category: 2.1 - Object Permissions
Condition(s):	SANS Storage Device	e: SANS Switch
Target(s):	SANS Storage Device	e; SANS Switch
Vulnerability	The zoning tables or	all affected HBAs are not reset (force a state change update) after making zoning changes.
	old addresses, which practice is to force a	ating devices also store a copy of the ACL. It is possible for the zoning information stored on the HBA to include are no longer allowed in the newly established zoning rules. The HBA's memory is non-persistent, thus a good state change update in the affected HBAs immediately after making zoning changes. sure that the zoning tables on all affected HBAs are reset (force a state change update) after making zoning
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:		D: The reviewer will interview the IAO/NSO to validate that the zoning tables on all affected HBAs are reset (force a patter making zoning changes. This reset is a manual activity so the interview is to find that the IAO/NSO is aware and does it.
Fix(es):	SPAN SAN03.005.00 zoning configuration	2: Develop and document a procedure to reset (force a state change update) all effected HBAs whenever SAN changes are made.
Notes: SAN04.001.00	CAT: 3	SAN devices not added to the site SSAA
	-	
8500.2 IA Control:	SANS Storage Device	Category: 12.2 - SSAA Doccumentation
	SANS Storage Device	
	_	added to the site System Security Authorization Agreement (SSAA).
Vulnerability	All hardware and sof have reviewed the in	tware will be entered into the SSAA. This gives a central location where it can be shown that all interested parties apact on their security posture and approved the implementation of the SAN. sure that SAN devices are added to the site System Security Authorization Agreement (SSAA).
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:	SPAN SAN04.001.00 Authorization Agreer	2: The reviewer will interview the IAO/NSO to validate that SAN devices are added to the site System Security nent (SSAA).
Fix(es):	SPAN SAN04.001.0	2: Update the SSAA following the SSAA review and acceptance procedures to include the SAN.
OPE	N: NO	A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		

SAN04.002.00

SAN04.002.00	CAT: 2	Compliance v	with Network	Infrastruct	ure and E	nclave	
3500.2 IA Control:	DCCS-1: DCCS-2		Category:	12.7 - Self-Asse	essment		
Condition(s):	SANS Storage Device	: SANS Switch					
Target(s):	SANS Storage Device	; SANS Switch					
Vulnerability	The SANs are not con the Network Infrastruc			ture, appropriate	enclave, and da	ta center security	y requirements in
	Inconsistencies with the vulnerabilities in the new The IAO/NSO will ensigned security requirements	etwork or the enclave. ure that SANs are com	pliant with overall net	work security arc	·		
References:	SHARING PERIPHER	ALS ACROSS THE N	ETWORK SECURITY	TECHNICAL IM	PLEMENTATIO	N GUIDE	
Checks:	SPAN SAN04.002.00: architecture, appropria						
Fix(es):	SPAN SAN04.002.00: formal review with FS0		sment with the Netwo	rk Infrastructure c	checklist and the	Enclave checkli	st or schedule a
OPE	in: NOI	A FINDING:	NOTRE	VIEWED:		Γ APPLICA	
Notes:	.N: NOT	A FINDING: [NOTRE	VIEWED:			
<u> </u>	CAT: 2	A FINDING:					
Notes:	CAT: 2		elated patche		nstalled.		
Notes: 6AN04.003.00 8500.2 IA Control:	CAT: 2	All security r	elated patche	s are not ir	nstalled.		
Notes: SAN04.003.00 3500.2 IA Control: Condition(s):	CAT: 2	All security re	elated patche	s are not ir	nstalled.		
Notes: SAN04.003.00 B500.2 IA Control: Condition(s): Target(s):	CAT: 2 VIVM-1 SANS Storage Device	All security research sans Switch	elated patche	s are not ir	nstalled.		
Notes: SAN04.003.00 3500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	CAT: 2 VIVM-1 SANS Storage Device SANS Storage Device	All security respectively. SANS Switch ches are not installed. ty related patches leave	elated patche Category:	S are not in 3.1 - Security Pa	nstalled. atches		
Notes: SAN04.003.00 B500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	CAT: 2 VIVM-1 SANS Storage Device SANS Storage Device All security related pat Failure to install secur	All security researches are not installed. ty related patches leavage that all security-related.	elated patche Category:	attack by exploitinalled.	nstalled. atches	abilities.	
Notes: SAN04.003.00 3500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	CAT: 2 VIVM-1 SANS Storage Device SANS Storage Device All security related pat Failure to install secur The IAO/NSO will ens	All security research security related patches leavure that all security-related ALS ACROSS THE N	elated patche Category: ves the SAN open to a lated patches are instale ETWORK SECURITY	es are not in 3.1 - Security Pa attack by exploitinalled.	nstalled. atches	abilities. N GUIDE	
Notes: SAN04.003.00 B500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	CAT: 2 VIVM-1 SANS Storage Device SANS Storage Device All security related pat Failure to install secur The IAO/NSO will ens SHARING PERIPHER	All security researches sand switch ches are not installed. ty related patches leaver that all security-related all security-related all security-related for the reviewer will, with after verifying that the	elated patche Category: ves the SAN open to a ated patches are insta ETWORK SECURITY in the assistance of the	es are not in 3.1 - Security Parattack by exploitinalled. TECHNICAL IM e IAO/NSO, verifyersely impact the	nstalled. atches ng known vulnera PLEMENTATIO y that all security production SAN	abilities. N GUIDE related patches	are installed.

8500.2 IA Control: DCCS-1: DCCS-2 Category: 12.7 - Self-Assessment Condition(s): SANS Storage Device: SANS Switch Target(s): SANS Storage Device; SANS Switch Vulnerability Prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructur are not configured to meet the applicable STIG requirements. Vulnerability Discussion: Many SAN components (servers, switches, management stations) have security requirements from other STIGs. It was all requirement are complied with. The IAO/NSO will ensure that prior to installing SAN components (servers, switches, and management stations) onto infrastructure, components are configured to meet the applicable STIG requirements. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.004.00: The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN constructions onto the DOD network infrastructure, components are configured to measure stations) onto the DOD network infrastructure, components are configured to measure stations. Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component devices reviewer or request a formal review from FSO.	will be verified that o the DOD network
Target(s): SANS Storage Device; SANS Switch Vulnerability Prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructur are not configured to meet the applicable STIG requirements. Vulnerability Discussion: Many SAN components (servers, switches, management stations) have security requirements from other STIGs. It was all requirement are complied with. The IAO/NSO will ensure that prior to installing SAN components (servers, switches, and management stations) onto infrastructure, components are configured to meet the applicable STIG requirements. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.004.00: The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN configured to meet the synthesis, and management stations) onto the DOD network infrastructure, components are configured to meet the synthesis and management stations onto the DOD network infrastructure, components are configured to meet the synthesis and management stations onto the DOD network infrastructure, components are configured to meet the applicable checklists or scripts on any component devices. Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component devices.	will be verified that o the DOD network
 Vulnerability Prior to installing SAN components (servers, switches, and management stations) onto the DOD network infrastructure are not configured to meet the applicable STIG requirements. Vulnerability Discussion: Many SAN components (servers, switches, management stations) have security requirements from other STIGs. It was all requirement are complied with. The IAO/NSO will ensure that prior to installing SAN components (servers, switches, and management stations) onto infrastructure, components are configured to meet the applicable STIG requirements. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.004.00: The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN configured to meet the applicable checklists or scripts on any component devices. Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component devices. 	will be verified that o the DOD network
are not configured to meet the applicable STIG requirements. Vulnerability Discussion: Many SAN components (servers, switches, management stations) have security requirements from other STIGs. It was all requirement are complied with. The IAO/NSO will ensure that prior to installing SAN components (servers, switches, and management stations) onto infrastructure, components are configured to meet the applicable STIG requirements. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.004.00: The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN configured to meaning stations of the DOD network infrastructure, components are configured to meaning the stations. Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component devices.	will be verified that o the DOD network
Discussion: all requirement are complied with. The IAO/NSO will ensure that prior to installing SAN components (servers, switches, and management stations) onto infrastructure, components are configured to meet the applicable STIG requirements. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.004.00: The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN co (servers, switches, and management stations) onto the DOD network infrastructure, components are configured to me STIG requirements. Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component devices.	o the DOD network
 Checks: SPAN SAN04.004.00: The reviewer will interview the IAO/NSO and view VMS to verify that prior to installing SAN co (servers, switches, and management stations) onto the DOD network infrastructure, components are configured to me STIG requirements. Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component devices. 	
(servers, switches, and management stations) onto the DOD network infrastructure, components are configured to me STIG requirements.Fix(es): SPAN SAN04.004.00: Perform a self assessment using the applicable checklists or scripts on any component devices.	
	e that has not been
OPEN: NOT A FINDING: NOT REVIEWED: NOT APPLICA	BLE:
Notes:	
SAN04.005.00 CAT: 2 Servers and hosts OS STIG Requirements	
8500.2 IA Control: DCCS-1: DCCS-2 Category: 12.7 - Self-Assessment	
Condition(s): SANS Storage Device: SANS Switch	
Target(s): SANS Storage Device; SANS Switch	
Vulnerability Servers and other hosts are not compliant with applicable Operating System (OS) STIG requirements.	
Vulnerability SAN servers and other hosts are hardware software combinations that actually run under the control of a native OS for component. This OS may be UNIX, LNIX, Windows, etc. The underlying OS must be configured to be compliant with STIG to ensure that they do not insert known vulnerabilities into the DOD network infrastructure. The IAO/NSO will ensure that servers and other hosts are compliant with applicable Operating System (OS) STIG recompositions.	th the applicable
References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE	
Checks: SPAN SAN04.005.00: The reviewer will interview the IAO/NSO and view the VMS to verify that servers and other hos with applicable Operating System (OS) STIG requirements.	osts are compliant
Fix(es): SPAN SAN04.005.00: Perform a self assessment using the applicable OS checklists or scripts on any server or host has not been reviewer or request a formal review from FSO.	st in the SAN that
	BLE:
OPEN: NOT A FINDING: NOT REVIEWED: NOT APPLICA	

SAN04.006.00	CAT: 1	Anti-virus on servers and host.
8500.2 IA Control:	ECVP-1	Category: 14.7 - Antivirus
Condition(s):	SANS Storage Device	e: SANS Switch
Target(s):	SANS Storage Device	e; SANS Switch
Vulnerability		OD approved, anti-virus software is not installed and configured on all SAN servers in accordance with the system STIG on SAN servers and management devices and kept up-to-date with the most recent virus definition
	not installed or the vi known vulnerabilities The IAO/NSO will en	sure that vendor supported, DOD approved, anti-virus software is installed and configured on all SAN servers in applicable operating system STIG on SAN servers and management devices and kept up-to-date with the most
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:	all SAN servers in ac date with the most re	The reviewer will verify that vendor supported, DOD approved, anti-virus software is installed and configured on cordance with the applicable operating system STIG on SAN servers and management devices and kept up-to-cent virus definition tables. If an OS review has reciently been completed verify that the anti-virus check was not a erform a manual check as described in the applicable OS checklist.
Fix(es):	SPAN SAN04.006.00	: Install and correctly configure a DOD approved anti-virus.
OPE Notes:	N: NOT	A FINDING: NOT REVIEWED: NOT APPLICABLE:
	217	
SAN04.007.00	CAT: 2	SAN Topology Drawing
8500.2 IA Control:		
Condition(s):	DCHW-1	Category: 12.9 - Documentation
Target(s):	DCHW-1 SANS Storage Device	· ·
rangon(o).		e: SANS Switch
• , ,	SANS Storage Device SANS Storage Device	e: SANS Switch
Vulnerability Vulnerability	SANS Storage Device SANS Storage Device A current drawing of being maintained. A drawing of the SAN in diagnosing potenti	e: SANS Switch the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment is not all topology gives the IAO and other interested individuals a pictorial representation of the SAN. This can be helpful all security problems. Intain a current drawing of the site's SAN topology that includes all external and internal links, zones, and all
Vulnerability Vulnerability Discussion:	SANS Storage Device SANS Storage Device A current drawing of being maintained. A drawing of the SAN in diagnosing potential The IAO/NSO will mainterconnected equip	e: SANS Switch the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment is not all topology gives the IAO and other interested individuals a pictorial representation of the SAN. This can be helpful all security problems. Intain a current drawing of the site's SAN topology that includes all external and internal links, zones, and all
Vulnerability Vulnerability Discussion: References:	SANS Storage Device SANS Storage Device A current drawing of being maintained. A drawing of the SAN in diagnosing potenti The IAO/NSO will mainterconnected equip SHARING PERIPHE SPAN SA04.007.00:	e: SANS Switch the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment is not a topology gives the IAO and other interested individuals a pictorial representation of the SAN. This can be helpful al security problems. intain a current drawing of the site's SAN topology that includes all external and internal links, zones, and all ment.
Vulnerability Vulnerability Discussion: References: Checks:	SANS Storage Device SANS Storage Device A current drawing of being maintained. A drawing of the SAN in diagnosing potential The IAO/NSO will mainterconnected equipments SHARING PERIPHE SPAN SA04.007.00: site's SAN topology to	e: SANS Switch the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment is not littopology gives the IAO and other interested individuals a pictorial representation of the SAN. This can be helpful all security problems. Intrain a current drawing of the site's SAN topology that includes all external and internal links, zones, and all ment. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE The reviewer will interview the IAO/NSO and view the drawings supplied to verify that a current drawing of the nat includes all external and internal links, zones, and all interconnected equipment. Create drawing of the site's SAN topology that includes all external and internal links, zones, and all
Vulnerability Vulnerability Discussion: References: Checks:	SANS Storage Device SANS Storage Device SANS Storage Device A current drawing of being maintained. A drawing of the SAN in diagnosing potenti The IAO/NSO will mainterconnected equip SHARING PERIPHE SPAN SA04.007.00: site's SAN topology to SPAN SAN04.007.00 interconnected equip	e: SANS Switch the site's SAN topology that includes all external and internal links, zones, and all interconnected equipment is not littopology gives the IAO and other interested individuals a pictorial representation of the SAN. This can be helpful all security problems. Intrain a current drawing of the site's SAN topology that includes all external and internal links, zones, and all ment. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE The reviewer will interview the IAO/NSO and view the drawings supplied to verify that a current drawing of the nat includes all external and internal links, zones, and all interconnected equipment. Create drawing of the site's SAN topology that includes all external and internal links, zones, and all

SAN04.008.00	CAT: 2 Physical Access to SAN Network Devices	
8500.2 IA Control:	PECF-1: PECF-2 Category: 5.9 - Device Locations	
Condition(s):	SANS Storage Device: SANS Switch	
Target(s):	SANS Storage Device; SANS Switch	
Vulnerability	All the network level devices interconnected to the SAN are not located in a secure room with limited access.	
	If the network level devices are not located in a secure area they can be tampered with which could lead to a denial of service if the device is powered off or sensitive data can be compromised by a tap connected to the device. The IAO/NSO will ensure that all the network level devices interconnected to the SAN are located in a secure room with limited access.	ess.
References:	SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE	
Checks:	SPAN SAN04.008.00: The reviewer will interview the IAO/NSO and view the network level devices to verify whether they are located a secure room with limited access.	d in
Fix(es):	SPAN SAN04.008.00: Develop a plan to move the network level devices to a location/room where the can be physically secured in a manner appropriate to the classification level of the data the handle. Obtain CM approval of the plan and then implement the plan moving the devices.	a
OPE	N: NOT A FINDING: NOT REVIEWED: NOT APPLICABLE:]
Notes:		
SAN04.009.00	CAT: 2 SAN Fabric Switch User Accounts with Passwords	
8500.2 IA Control:	IAIA-1: IAIA-2 Category: 1.3 - Identity Management	
` ,		
	SANS Switch: SANS Storage Device	
• • • • • • • • • • • • • • • • • • • •	SANS Storage Device; SANS Switch	
Vulnerability	SANS Storage Device; SANS Switch Individual user accounts with passwords are not set up and maintained for the SAN fabric switch.	
Vulnerability Vulnerability	SANS Storage Device; SANS Switch	e
Vulnerability Vulnerability Discussion:	SANS Storage Device; SANS Switch Individual user accounts with passwords are not set up and maintained for the SAN fabric switch. Without identification and authentication unauthorized users could reconfigure the SAN or disrupt its operation by logging in to the fabric switch and executing unauthorized commands. The IAO/NSO will ensure individual user accounts with passwords are set up and maintained for the SAN fabric switch in accordance.	
Vulnerability Vulnerability Discussion: References:	SANS Storage Device; SANS Switch Individual user accounts with passwords are not set up and maintained for the SAN fabric switch. Without identification and authentication unauthorized users could reconfigure the SAN or disrupt its operation by logging in to the fabric switch and executing unauthorized commands. The IAO/NSO will ensure individual user accounts with passwords are set up and maintained for the SAN fabric switch in accordance with the guidance contained in Appendix B, CJCSM and the Network Infrastructure STIG. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran: SHARING PERIPHERALS	S
Vulnerability Vulnerability Discussion: References: Checks:	SANS Storage Device; SANS Switch Individual user accounts with passwords are not set up and maintained for the SAN fabric switch. Without identification and authentication unauthorized users could reconfigure the SAN or disrupt its operation by logging in to the fabric switch and executing unauthorized commands. The IAO/NSO will ensure individual user accounts with passwords are set up and maintained for the SAN fabric switch in accordance with the guidance contained in Appendix B, CJCSM and the Network Infrastructure STIG. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE SPAN SA04.009.00: The reviewer, with the assistance of the IAO/NSO, will verify that individual user accounts with passwords are standard to the same passwords are standard to the same passwords.	S set
Vulnerability Vulnerability Discussion: References: Checks:	SANS Storage Device; SANS Switch Individual user accounts with passwords are not set up and maintained for the SAN fabric switch. Without identification and authentication unauthorized users could reconfigure the SAN or disrupt its operation by logging in to the fabric switch and executing unauthorized commands. The IAO/NSO will ensure individual user accounts with passwords are set up and maintained for the SAN fabric switch in accordance with the guidance contained in Appendix B, CJCSM and the Network Infrastructure STIG. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE SPAN SA04.009.00: The reviewer, with the assistance of the IAO/NSO, will verify that individual user accounts with passwords are sup and maintained for the SAN fabric switch. SPAN SA04.009.00: Develop a plan to reconfigure the SAN fabric switch to require user accounts and passwords. This plan also needs to include the creation and distribution of user accounts and passwords for each administrator who requires access to the SAN fabric switch. Obtain CM approval of the plan and then implement the plan.	S set
Vulnerability Vulnerability Discussion: References: Checks: Fix(es):	SANS Storage Device; SANS Switch Individual user accounts with passwords are not set up and maintained for the SAN fabric switch. Without identification and authentication unauthorized users could reconfigure the SAN or disrupt its operation by logging in to the fabric switch and executing unauthorized commands. The IAO/NSO will ensure individual user accounts with passwords are set up and maintained for the SAN fabric switch in accordance with the guidance contained in Appendix B, CJCSM and the Network Infrastructure STIG. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE SPAN SA04.009.00: The reviewer, with the assistance of the IAO/NSO, will verify that individual user accounts with passwords are sup and maintained for the SAN fabric switch. SPAN SA04.009.00: Develop a plan to reconfigure the SAN fabric switch to require user accounts and passwords. This plan also needs to include the creation and distribution of user accounts and passwords for each administrator who requires access to the SAN fabric switch. Obtain CM approval of the plan and then implement the plan.	S set

SAN04.010.00 CAT: 3 Sensitive Data in Transit Encryption 8500.2 IA Control: ECNK-1 Category: 8.1 - Encrypted Data in Transit Condition(s): SANS Storage Device: SANS Switch Target(s): SANS Storage Device; SANS Switch Vulnerability All fabric switches for SANs that process sensitive information are not configured to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications. Vulnerability It is necessary to protect the confidentiality of sensitive data in transit over a network that is used to transmit other sensitive data that Discussion: has a differing need-to-know criteria. The IAO/NSO will configure all fabric switches to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications for SANs that process sensitive information. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.010.00: The reviewer will, with the assistance of the IAO/NSO, verify that all fabric switches are configured to use a FIPS 140-1/2 validated algorithm to encrypt switch-to-switch communications for SANs that process sensitive information. Fix(es): SPAN SAN04.010.00: Develop a plan to reconfigure the SAN fabric switches to use FIPS-140-1/2 validated algorithms to encrypt switch-to-switch communications for SANs that process sensitive information. Obtain CM approval for the plan and then implement the plan. OPEN: **NOT A FINDING:** NOT REVIEWED: **NOT APPLICABLE:** Notes: SAN04.011.00 CAT: 3 SAN Switch encryption and DOD PKI 8500.2 IA Control: ECNK-1: IAIA-1: IAIA-2 Category: 1.3 - Identity Management Condition(s): SANS Storage Device: SANS Switch Target(s): SANS Storage Device; SANS Switch Vulnerability The fabric switches are not protected by encryption and DOD PKI and/or that the manufacturer's default keys have not been changed prior to attaching to the SAN Fabric for SANs processing sensitive information... Vulnerability Failure to provide encryption for SAN switches that handle sensitive data can lead to the compromise of sensitive data. DOD PKI will Discussion: supplies better protection from malicious attacks than userid/password authentication and should be used anytime it is feasible. If manufactures default keys are not changed prior to connection to the network the switch will be vulnerable to malicious attacks by individuals who know these keys. The IAO/NSO will ensure that fabric switches are protected by encryption and DOD PKI and that the manufacturer's default keys are changed prior to attaching to the SAN Fabric for SANs processing sensitive information. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.011.00: The reviewer will, with the assistance of the IAO/NSO, verify that fabric switches are protected by encryption and DOD PKI and that the manufacturer's default keys are changed prior to attaching to the SAN Fabric for SANs processing sensitive information. Fix(es): SPAN SAN04.011.00: Develop a plan to implement encryption, DOD PKI and change the manufacturers default keys. Obtain CM approval for the plan and then execute the plan. **NOT REVIEWED:** OPEN: NOT A FINDING: NOT APPLICABLE: Notes:

SAN04.012.00

AN04.012.00	CAT: 2	SAN Network Management Ports Fabric Switch
500.2 IA Control:	DCBP-1	Category: 14.4 - Unneeded Ports, Protocols, Hardware, and Services
Condition(s):	SANS Switch	
Target(s):	SANS Switch	
Vulnerability	Network management not disabled.	nt ports on the SAN fabric switches except those needed to support the operational commitments of the sites are
	vulnerabilities. By dis	nagement ports that are not required expose the SAN fabric switch and the entire network to unnecessary sabling these unneeded ports the exposure profile of the device and network is diminished. sable all network management ports on the SAN fabric switches except those needed to support the operational sites.
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:		D: The reviewer will, with the assistance of the IAO/NSO, verify that all network management ports on the SAN isabled except those needed to support the operational commitments of the sites.
Fix(es):		Develop a plan to locate and disable all network management ports that are not required to support the lents of the sites. Obtain CM approval of the plan and then execute the plan.
OPE Notes:		
Notes:	CAT: 2	SAN management out-of-band or direct connect
Notes:		SAN management out-of-band or direct connect Category: 14.5 - Physical Layer Security
Notes: AN04.013.00 500.2 A Control:		Category: 14.5 - Physical Layer Security
Notes: AN04.013.00 500.2 IA Control: Condition(s):	DCBP-1	Category: 14.5 - Physical Layer Security se: SANS Switch
AN04.013.00 500.2 IA Control: Condition(s): Target(s):	DCBP-1 SANS Storage Devic SANS Storage Devic	Category: 14.5 - Physical Layer Security se: SANS Switch
AN04.013.00 500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	DCBP-1 SANS Storage Devic SANS Storage Devic SAN management is Removing the management ports to	Category: 14.5 - Physical Layer Security re: SANS Switch re; SANS Switch
Notes: AN04.013.00 500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	DCBP-1 SANS Storage Devic SANS Storage Devic SAN management is Removing the management ports to The IAO/NSO will en	Category: 14.5 - Physical Layer Security ee: SANS Switch ee: SANS Switch accomplished using the out-of-band or direct connection method. gement traffic from the production network diminishes the security profile of the SAN servers by allowing all the be closed on the production network.
Notes: AN04.013.00 500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	DCBP-1 SANS Storage Device SANS Storage Device SAN management is Removing the management ports to The IAO/NSO will ensemble SHARING PERIPHER	Category: 14.5 - Physical Layer Security se: SANS Switch se; SANS Switch accomplished using the out-of-band or direct connection method. gement traffic from the production network diminishes the security profile of the SAN servers by allowing all the obe closed on the production network. sure that SAN management is accomplished using the out-of-band or direct connection method.
Notes: SAN04.013.00 S500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	DCBP-1 SANS Storage Devic SANS Storage Devic SAN management is Removing the management ports to The IAO/NSO will en	Category: 14.5 - Physical Layer Security se: SANS Switch se; SANS Switch accomplished using the out-of-band or direct connection method. gement traffic from the production network diminishes the security profile of the SAN servers by allowing all the obe closed on the production network. sure that SAN management is accomplished using the out-of-band or direct connection method.
Notes: SAN04.013.00 S500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	DCBP-1 SANS Storage Device SANS Storage Device SAN management is Removing the managemanagement ports to The IAO/NSO will ensign SHARING PERIPHEI SPAN SAN04.013.00 CM approval for the paragement ports to the IAO/NSO will ensign sharing period of the paragement of t	Category: 14.5 - Physical Layer Security se: SANS Switch se; SANS Switch accomplished using the out-of-band or direct connection method. gement traffic from the production network diminishes the security profile of the SAN servers by allowing all the be closed on the production network. sure that SAN management is accomplished using the out-of-band or direct connection method. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

SAN04.014.00	CAT: 3	Management Console to SAN Fabric DOD PKI protected
8500.2 IA Control:	IAIA-1: IAIA-2	Category: 1.2 - PKI
Condition(s):	SANS Storage Device	ce: SANS Switch
Target(s):	SANS Storage Device	ce; SANS Switch
Vulnerability	Communications fro	m the management console to the SAN fabric are not protected using DOD PKI.
	carrying privileged fu	nentication between the SAN management console and the fabric enhances the security of the communications unctions. It is harder for an unauthorized management console to take control of the SAN. Is a sure that communications from the management console to the SAN fabric are protected using DOD PKI.
References:	SHARING PERIPHE	ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE
Checks:		0: The reviewer will, with the assistance of the IAO/NSO, verify that communications from the management fabric are protected using DOD PKI.
Fix(es):		0: Develop a plan to migrate to the use of DOD PKI authentication between the SAN management console and the CM approval of the plan and implement the plan.
OPE	N: NO	T A FINDING: NOT REVIEWED: NOT APPLICABLE:
Notes:		
SAN04.015.00	CAT: 3	Default PKI keys
SAN04.015.00 8500.2 IA Control:		Default PKI keys Category: 1.2 - PKI
		Category: 1.2 - PKI
8500.2 IA Control: Condition(s):	IAIA-1: IAIA-2	Category: 1.2 - PKI
8500.2 IA Control: Condition(s): Target(s):	IAIA-1: IAIA-2 SANS Storage Devid SANS Storage Devid	Category: 1.2 - PKI
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device The manufacturer's If the manufacturer's access to the default	Category: 1.2 - PKI ce: SANS Switch ce; SANS Switch default PKI keys have not been changed prior to attaching the switch to the SAN Fabric. default PKI keys are allowed to remain active on the device, it can be accessed by a malicious individual with
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device The manufacturer's If the manufacturer's access to the defaul The IAO/NSO will er	Category: 1.2 - PKI ce: SANS Switch ce; SANS Switch default PKI keys have not been changed prior to attaching the switch to the SAN Fabric. default PKI keys are allowed to remain active on the device, it can be accessed by a malicious individual with t key.
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device The manufacturer's access to the defaulthe IAO/NSO will er SHARING PERIPHE SPAN SAN04.015.0	Category: 1.2 - PKI ce: SANS Switch ce; SANS Switch default PKI keys have not been changed prior to attaching the switch to the SAN Fabric. default PKI keys are allowed to remain active on the device, it can be accessed by a malicious individual with t key. Insure that the manufacturer's default PKI keys are changed prior to attaching the switch to the SAN Fabric.
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device The manufacturer's access to the defaulthe IAO/NSO will er SHARING PERIPHE SPAN SAN04.015.0 changed prior to attas SPAN SAN04.015.0	Category: 1.2 - PKI ce: SANS Switch ce; SANS Switch default PKI keys have not been changed prior to attaching the switch to the SAN Fabric. default PKI keys are allowed to remain active on the device, it can be accessed by a malicious individual with t key. Insure that the manufacturer's default PKI keys are changed prior to attaching the switch to the SAN Fabric. ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE 0: The reviewer will, with the assistance of the IAO/NSO, verify that the manufacturer's default PKI keys have been
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device The manufacturer's If the manufacturer's access to the defaul The IAO/NSO will er SHARING PERIPHE SPAN SAN04.015.0 changed prior to atta SPAN SAN04.015.0 manufacturer's defau implement the plan.	Category: 1.2 - PKI ce: SANS Switch ce; SANS Switch default PKI keys have not been changed prior to attaching the switch to the SAN Fabric. default PKI keys are allowed to remain active on the device, it can be accessed by a malicious individual with t key. Insure that the manufacturer's default PKI keys are changed prior to attaching the switch to the SAN Fabric. ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will, with the assistance of the IAO/NSO, verify that the manufacturer's default PKI keys have been aching the switch to the SAN Fabric. O: Depending on the functionality allowed by the device, develop a plan remove, disable or change the

SAN04.016.00

CAT: **3**

SAN04.016.00	CAT: 3	FIPS 140-1/2 for management to fabric.				
8500.2 IA Control:	ECNK-1 Category: 8.1 - Encrypted Data in Transit					
Condition(s):	SANS Switch: SANS Storage Device					
Target(s):	SANS Storage Device; SANS Switch					
Vulnerability	The SAN is not configured to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.					
	The communication between the SAN management consol and the SAN fabric carries sensitive privileged configuration data. This data's confidentiality will be protected with FIPS 140-1/2 validate algorithm for encryption. Configuration data could be used to create a denial of service by disrupting the SAN fabric. The storage administrator will configure the SAN to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.					
References:	SHARING PERIPHE	RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE				
Checks:	SPAN SAN04.016.00: The reviewer will, with the assistance of the storage administrator, verify that the SAN is configured to use FIPS 140-1/2 validated encryption algorithm to protect management-to-fabric communications.					
Fix(es):	SPAN SA04.016.00: Develop a plan to implement FIPS-140-1/2 validated encryption to protect management-to-fabric communications. Obtain CM approval of the plan and execute the plan.					
ОРЕ	EN: NOT	A FINDING: NOT REVIEWED: NOT APPLICABLE:				
Notes:						
SAN04.017.00	CAT: 1	Password SAN Management Console and Ports				
	-	Password SAN Management Console and Ports Category: 1.3 - Identity Management				
8500.2 IA Control:	IAIA-1: IAIA-2	Category: 1.3 - Identity Management				
8500.2 IA Control: Condition(s):	-	Category: 1.3 - Identity Management se: SANS Switch				
8500.2 IA Control: Condition(s): Target(s):	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device	Category: 1.3 - Identity Management se: SANS Switch				
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device All SAN management Without password predate by reconfiguring	Category: 1.3 - Identity Management ee: SANS Switch ee; SANS Switch				
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device All SAN management Without password predate by reconfiguring The IAO/NSO will en	Category: 1.3 - Identity Management ce: SANS Switch ce: SANS Switch at consoles and ports are not password protected. otection malicious users can create a denial of service by disrupting the SAN or allow the compromise of sensitive of the SAN topography.				
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device All SAN management Without password predate by reconfiguring The IAO/NSO will ent SHARING PERIPHE	Category: 1.3 - Identity Management ce: SANS Switch ce; SANS Switch ct consoles and ports are not password protected. otection malicious users can create a denial of service by disrupting the SAN or allow the compromise of sensitive of the SAN topography. Issure that all SAN management consoles and ports are password protected.	•			
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device All SAN management Without password predate by reconfiguring The IAO/NSO will ent SHARING PERIPHE SPAN SAN04.017: password protected. SPAN SAN04.017.00	Category: 1.3 - Identity Management ce: SANS Switch ce; SANS Switch ct consoles and ports are not password protected. otection malicious users can create a denial of service by disrupting the SAN or allow the compromise of sensitive of the SAN topography. Issure that all SAN management consoles and ports are password protected. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE	•			
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	IAIA-1: IAIA-2 SANS Storage Device SANS Storage Device All SAN management Without password predate by reconfiguring The IAO/NSO will ent SHARING PERIPHE SPAN SAN04.017: password protected. SPAN SAN04.017.00 CM approval of the password protection	Category: 1.3 - Identity Management ce: SANS Switch ce: SANS Switch ct consoles and ports are not password protected. otection malicious users can create a denial of service by disrupting the SAN or allow the compromise of sensitive of the SAN topography. sure that all SAN management consoles and ports are password protected. CRALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE The reviewer will, with the assistance of the IAO/NSO, verify that all SAN management consoles and ports are D: Develop a plan for implementing password protection on the SAN's management consoles and ports. Obtain	•			

SAN04.018.00	CAT: 1	Default SAN Management Software Password				
8500.2 IA Control:	IAIA-1: IAIA-2	Category: 1.3 - Identity Management				
Condition(s):	SANS Storage Device: SANS Switch					
Target(s):	SANS Storage Device; SANS Switch					
Vulnerability	The manufacturer's default passwords have not been changed for all SAN management software.					
	The changing of passwords from the default value blocks malicious users with knowledge of the default passwords for the manufacturer's SAN Management software from creating a denial of service by disrupting the SAN or reconfigure the SAN topology leading to a compromise of sensitive data. The IAO/NSO will ensure that the manufacturer's default passwords are changed for all SAN management software.					
References:	SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE					
Checks:	SPAN SAN04.018.00: The reviewer will, with the assistance of the IAO/NSO, verify that the manufacturer's default passwords have been changed for all SAN management software.					
Fix(es):		: Develop a plan to change manufacturer's default passwords for all SAN management software. Obtain CM nd implement the plan.				
OPE Notes:	N: NOT	A FINDING: NOT REVIEWED: NOT APPLICABLE:				
SAN04.019.00	CAT: 1	SAN Fabric Zoning List Deny-By-Default				
8500.2 IA Control:	DCBP-1	Outcome OA Object Provide in				
Condition(s):	SANS Storage Device: SANS Switch					
Target(s):	SANS Storage Device	Category: 2.1 - Object Permissions e: SANS Switch				
Vulnerability	SANS Storage Device	e: SANS Switch				
	SANS Storage Device	e: SANS Switch e; SANS Switch g lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the				
Vulnerability	SANS Storage Device The SAN fabric zonin given port or by the s By using the Deny-by denied access. If De access to sensitive de The IAO/NSO will ens	e: SANS Switch e; SANS Switch g lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the				
Vulnerability Discussion:	SANS Storage Device The SAN fabric zonin given port or by the s By using the Deny-by denied access. If De access to sensitive da The IAO/NSO will ens not required on the gi	e: SANS Switch g lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the te. -Default based policy, any service or protocol not required by a port and overlooked in the zoning list will be ny-by-Default based policy was not used any overlooked service or protocol not required by a port could have at a compromising that data. sure that SAN fabric zoning lists are based on a policy of Deny-by-Default with blocks on all services and protocols				
Vulnerability Discussion: References:	SANS Storage Device The SAN fabric zonin given port or by the s By using the Deny-by denied access. If De access to sensitive dracess to sensitive draces to sensitive draces and required on the gi SHARING PERIPHEI SPAN SAN04.019.00	e: SANS Switch g lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the te. -Default based policy, any service or protocol not required by a port and overlooked in the zoning list will be ny-by-Default based policy was not used any overlooked service or protocol not required by a port could have ata compromising that data. sure that SAN fabric zoning lists are based on a policy of Deny-by-Default with blocks on all services and protocols wen port or by the site.				
Vulnerability Discussion: References: Checks:	SANS Storage Device The SAN fabric zonin given port or by the s By using the Deny-by denied access. If De access to sensitive denied access to sensitive den	e: SANS Switch g lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the te. -Default based policy, any service or protocol not required by a port and overlooked in the zoning list will be hy-by-Default based policy was not used any overlooked service or protocol not required by a port could have at a compromising that data. Sure that SAN fabric zoning lists are based on a policy of Deny-by-Default with blocks on all services and protocols over port or by the site. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE The reviewer will, with the assistance of the IAO/NSO, verify that SAN fabric zoning lists are based on a policy				
Vulnerability Discussion: References: Checks:	SANS Storage Device The SAN fabric zonin given port or by the s By using the Deny-by denied access. If De access to sensitive de The IAO/NSO will ens not required on the gi SHARING PERIPHEI SPAN SAN04.019.00 of Deny-by-Default w SPAN SAN04.019.00 enforce a Deny-by-De approval for the plan	e: SANS Switch g lists are not based on a policy of Deny-by-Default with blocks on all services and protocols not required on the te. -Default based policy, any service or protocol not required by a port and overlooked in the zoning list will be ny-by-Default based policy was not used any overlooked service or protocol not required by a port could have ata compromising that data. Sure that SAN fabric zoning lists are based on a policy of Deny-by-Default with blocks on all services and protocols wen port or by the site. RALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE The reviewer will, with the assistance of the IAO/NSO, verify that SAN fabric zoning lists are based on a policy the blocks on all services and protocols not required on the given port or by the site. Develop a plan to identify all services and protocols needed by each port in the SAN, modify the routing lists to a fault policy and allow only the identified services and protocols on each port that requires them. Obtain CM				

SAN04.020.00	CAT: 3	Logging Failed	Access to	Port, Protoc	cols, Services		
8500.2 IA Control:	ECAR-1: ECAR-2: ECA	R-3	Category:	10.2 - Content Co	onfiguration		
Condition(s):	SANS Storage Device: SANS Switch						
Target(s):	SANS Storage Device; SANS Switch						
Vulnerability	Attempts to access ports, protocols, or services that are denied are not logged						
	Logging or auditing of failed access attempts is a necessary component for the forensic investigation of security incidents. Without logging there is no way to demonstrate that the access attempt was made or when it was made. Additionally a pattern of access failures cannot be demonstrated to assert that an intended attack was being made as apposed to an accidental intrusion. The IAO/NSO will ensure that all attempts to any port, protocol, or service that is denied are logged.						
References:	SHARING PERIPHERA	SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE					
Checks:	SPAN SAN04.020.00: The reviewer will, with the assistance of the IAO/NSO, verify that all attempts to any port, protocol, or service that is denied are logged.						
Fix(es):	SPAN SAN04.020.00: Develop a plan to implement the logging of failed or rejected ports, protocols or services requests. The plan should include a projection of the storage requirements of the logged events. Obtain CM approval of the plan and execute it.						
ОРЕ	N: NOT A	FINDING:	NOT RE	VIEWED:	NOT APPLICABLE:		
Notes:							
SAN04.021.00	CAT: 2	SNMP usage ar	nd configur	ation.			
SAN04.021.00 8500.2 IA Control:	_	SNMP usage ar	•	ation. 14.2 - Protocol Se	ecurity		
8500.2 IA Control:	_	•	•		ecurity		
8500.2 IA Control: Condition(s):	DCBP-1	orage Device	•		ecurity		
8500.2 IA Control: Condition(s): Target(s):	DCBP-1 SANS Switch: SANS Sto SANS Storage Device;	orage Device SANS Switch ement Protocol (SNMP)	Category:	14.2 - Protocol Se	ecurity cordance with the guidance contained in the		
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	DCBP-1 SANS Switch: SANS Str SANS Storage Device; Simple Network Manage Network Infrastructure S There are vulnerabilities in the Network Infrastruc	orage Device SANS Switch ement Protocol (SNMP) TIG. in some implementation cture STIG in selecting a gement Protocol (SNMF)	Category: is used and it is not and some confiversion of SNMP	14.2 - Protocol Se ot configured in acc gurations of SNMP to use and how to	,		
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	DCBP-1 SANS Switch: SANS Str SANS Storage Device; Simple Network Manage Network Infrastructure S There are vulnerabilities in the Network Infrastruct If Simple Network Manage	orage Device SANS Switch ement Protocol (SNMP) TIG. in some implementation cture STIG in selecting a gement Protocol (SNMP) k Infrastructure STIG.	Category: is used and it is not and some confictiversion of SNMP by is used, the IAO	14.2 - Protocol Se ot configured in acc gurations of SNMP to use and how to /NSO will ensure it	cordance with the guidance contained in the 2. Therefore if SMPT is used the guidelines found configure it will be followed. 3. is configured in accordance with the guidance		
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	DCBP-1 SANS Switch: SANS Storage Device; Simple Network Manage Network Infrastructure S There are vulnerabilities in the Network Infrastructure If Simple Network Manacontained in the Network SHARING PERIPHERA	orage Device SANS Switch ement Protocol (SNMP) TIG. in some implementation cture STIG in selecting a gement Protocol (SNMF) k Infrastructure STIG. LS ACROSS THE NETA	Category: is used and it is not as and some confit version of SNMP ') is used, the IAO WORK SECURITY e IAO/NSO, verify	ot configured in according and how to use and how to NSO will ensure it	cordance with the guidance contained in the P. Therefore if SMPT is used the guidelines found configure it will be followed. Is configured in accordance with the guidance LEMENTATION GUIDE Work Management Protocol (SNMP) is used, it is		
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	DCBP-1 SANS Switch: SANS Storage Device; Simple Network Manage Network Infrastructure S There are vulnerabilities in the Network Infrastructure If Simple Network Mana contained in the Network SHARING PERIPHERA SPAN SAN04.021.00: A configured in accordance.	orage Device SANS Switch ement Protocol (SNMP) TIG. in some implementation cture STIG in selecting a gement Protocol (SNMF) k Infrastructure STIG. LS ACROSS THE NET\ With the assistance of the e with the guidance con-	Category: is used and it is not and some confit version of SNMP by is used, the IAO WORK SECURITY e IAO/NSO, verify tained in the Netw	ot configured in according and to use and how to I/NSO will ensure it I/TECHNICAL IMPLICATION TO THE IMPLICA	cordance with the guidance contained in the P. Therefore if SMPT is used the guidelines found configure it will be followed. Is configured in accordance with the guidance LEMENTATION GUIDE Work Management Protocol (SNMP) is used, it is		
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	DCBP-1 SANS Switch: SANS Storage Device; Simple Network Manage Network Infrastructure S There are vulnerabilities in the Network Infrastructif Simple Network Manacontained in the Network SHARING PERIPHERA SPAN SAN04.021.00: Vaconfigured in accordance SPAN SAN04.021.00: If and execute the plan.	orage Device SANS Switch ement Protocol (SNMP) TIG. in some implementation cture STIG in selecting a gement Protocol (SNMF) k Infrastructure STIG. LS ACROSS THE NET\ With the assistance of the e with the guidance con-	Category: is used and it is not and some confit version of SNMP is used, the IAO WORK SECURITY e IAO/NSO, verify tained in the Netwo	ot configured in according and to use and how to I/NSO will ensure it I/TECHNICAL IMPLICATION TO THE IMPLICA	cordance with the guidance contained in the 2. Therefore if SMPT is used the guidelines found configure it will be followed. 3. is configured in accordance with the guidance LEMENTATION GUIDE Work Management Protocol (SNMP) is used, it is STIG section 5.1.2.		

SAN04.022.00	CAT: 1 Authorized IP Addresses allowed for SNMP					
8500.2 IA Control:	DCBP-1 Category: 14.2 - Protocol Security					
Condition(s):	SANS Storage Device: SANS Switch					
Target(s):	SANS Storage Device; SANS Switch					
Vulnerability	Unauthorized IP add	resses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices.				
	SNMP, by virtue of what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device parameters, unauthorized users can cause damage. Restricting IP address that can access SNMP on the SAN devices will further limit the possibility of malicious access being made. The IAO/NSO will ensure that only authorized IP addresses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices.					
References:	SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE					
Checks:	SPAN SAN04.022.00: The reviewer will, with the assistance of the IAO/NSO, verify that only authorized IP addresses are allowed Simple Network Management Protocol (SNMP) access to the SAN devices. This can be done with by checking the ACLs for the SAN device ports.					
Fix(es):	SPAN SAN04.022.00: Develop a plan to restrict SNMP access to SAN devices to authorized IP addresses. Obtain CM approval for the plan and implement the plan.					
ОРЕ	N: NO	T A FINDING: NOT REVIEWED: NOT APPLICABLE:				
Notes:						
SAN04.023.00	CAT: 2	Only Internal Network SNMP Access to SAN				
SAN04.023.00 8500.2 IA Control:		Only Internal Network SNMP Access to SAN Category: 2.1 - Object Permissions				
8500.2 IA Control:		Category: 2.1 - Object Permissions				
8500.2 IA Control: Condition(s):	EBRP-1	Category: 2.1 - Object Permissions ce: SANS Switch				
8500.2 IA Control: Condition(s): Target(s):	EBRP-1 SANS Storage Devid SANS Storage Devid	Category: 2.1 - Object Permissions ce: SANS Switch				
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability	EBRP-1 SANS Storage Device SANS Storage Device The IP addresses of SNMP, by virtue of v parameters, unauthor	Category: 2.1 - Object Permissions ce: SANS Switch ce; SANS Switch the hosts permitted SNMP access to the SAN management devices do not belong to the internal network. what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device orized users can cause damage. Therefore access to a SAN device from an IP address outside of the internal				
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion:	EBRP-1 SANS Storage Device SANS Storage Device The IP addresses of SNMP, by virtue of v parameters, unauthor network will not be at The IAO/NSO will er internal network.	Category: 2.1 - Object Permissions ce: SANS Switch ce; SANS Switch the hosts permitted SNMP access to the SAN management devices do not belong to the internal network. what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device orized users can cause damage. Therefore access to a SAN device from an IP address outside of the internal llowed.				
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References:	EBRP-1 SANS Storage Device SANS Storage Device The IP addresses of SNMP, by virtue of v parameters, unauthor network will not be a The IAO/NSO will er internal network. SHARING PERIPHE SPAN SAN04.023.0	Category: 2.1 - Object Permissions ce: SANS Switch ce; SANS Switch the hosts permitted SNMP access to the SAN management devices do not belong to the internal network. what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device prized users can cause damage. Therefore access to a SAN device from an IP address outside of the internal llowed. Issure IP addresses of the hosts that are permitted SNMP access to the SAN management devices belong to the				
8500.2 IA Control: Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	EBRP-1 SANS Storage Device SANS Storage Device The IP addresses of SNMP, by virtue of very parameters, unauthor network will not be at The IAO/NSO will er internal network. SHARING PERIPHE SPAN SAN04.023.0 access to the SAN in SPAN SAN04.023.0	Category: 2.1 - Object Permissions ce: SANS Switch ce: SANS Switch the hosts permitted SNMP access to the SAN management devices do not belong to the internal network. what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device orized users can cause damage. Therefore access to a SAN device from an IP address outside of the internal llowed. Issure IP addresses of the hosts that are permitted SNMP access to the SAN management devices belong to the ERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will, with the assistance of the IAO/NSO, verify that the IP addresses of the hosts permitted SNMP				
Condition(s): Target(s): Vulnerability Vulnerability Discussion: References: Checks:	EBRP-1 SANS Storage Device SANS Storage Device The IP addresses of SNMP, by virtue of very parameters, unauthor network will not be at the IAO/NSO will er internal network. SHARING PERIPHE SPAN SAN04.023.0 access to the SAN in SPAN SAN04.023.0 approval of the plan	Category: 2.1 - Object Permissions ce: SANS Switch the hosts permitted SNMP access to the SAN management devices do not belong to the internal network. what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device prized users can cause damage. Therefore access to a SAN device from an IP address outside of the internal llowed. Issure IP addresses of the hosts that are permitted SNMP access to the SAN management devices belong to the SAN SAN SECURITY TECHNICAL IMPLEMENTATION GUIDE O: The reviewer will, with the assistance of the IAO/NSO, verify that the IP addresses of the hosts permitted SNMP management devices belong to the internal network. The ACLs for the SAN ports should be checked. O: Develop a plan to restrict SNMP access to SAN devices to only internal network IP addresses. Obtain CM				

SAN04.024.00

CAT: 3

Fibre Channel network End-User Platform Restricted 8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions Condition(s): SANS Storage Device: SANS Switch Target(s): SANS Storage Device; SANS Switch Vulnerability End-user platforms are directly attached to the Fibre Channel network or access storage devices directly. Vulnerability End-user platforms should only be connected to servers that run applications that access the data found on the SAN devices. SANs do Discussion: not supply a robust user identification and authentication platform. They depend on the servers and applications to authenticate the users and restrict access to users as required. The IAO/NSO will ensure that end-user platforms are not directly attached to the Fibre Channel network and may not access storage devices directly. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.024.00: The reviewer will, with the assistance of the IAO/NSO, verify that end-user platforms are not directly attached to the Fibre Channel network and may not access storage devices directly. If the SAN is small with all of its components collocated, this can be done by a visual inspection but in most cases the reviewer will have to check the SAN network drawing. Fix(es): SPAN SAN04.024.00: Develop a plan to remove end-user platforms from the SAN. Obtain CM approval for the plan and implement the plan. OPEN: **NOT A FINDING:** NOT REVIEWED: **NOT APPLICABLE:** Notes: SAN04.025.00 CAT: 2 SAN Fixed IP Required. 8500.2 IA Control: DCBP-1 Category: 14.3 - Network Device Configuration Condition(s): SANS Storage Device: SANS Switch Target(s): SANS Storage Device; SANS Switch Vulnerability SAN components are not configured with fixed IP addresses. Vulnerability Without fixed IP address filtering or restricting of access based on IP addressing will not function correctly allowing unauthorized access Discussion: to SAN components or creating a denial of service by blocking legitimate traffic from authorized components. The storage administrator will ensure that all SAN components are configured to use static IP addresses. References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE Checks: SPAN SAN04.25.00: The reviewer with the assistance of the SA will verify that all SAN components are configured with fixed IP addresses. Fix(es): SPAN SAN04.025.00: Configure all SAN components to have fixed IP addresses. **NOT A FINDING: NOT REVIEWED: NOT APPLICABLE:** OPEN: Notes:

SAN05.001.00

CAT: 2

8500.2 IA Control: COSW-1 Category: 13.4 - Backup & Recovery Condition(s): SANS Storage Device: SANS Switch Target(s): SANS Storage Device; SANS Switch

Vulnerability Fabric switch configurations and management station configuration are not archived and/or copies of the operating system and other critical software for all SAN components are not stored in a fire rated container or are not collocated with the operational software.

Vulnerability .Backup and recovery procedures are critical to the security and availability of the SAN system. If a system is compromised, shut down, Discussion: or otherwise not available for service, this could hinder the availability of resources to the warfighter.

The IAO/NSO will ensure that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with

Backup of critical SAN Software and configurations

the operational software.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN SAN05.001.00: The reviewer will interview the IAO/NSO and view the stored information to verify that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with the operational software.

Fix(es): SPAN SAN05.001.00: Develop a plan that will ensure that all fabric switch configurations and management station configuration are archived and copies of the operating system and other critical software for all SAN components are stored in a fire rated container or otherwise not collocated with the operational software. Obtain CM approval for the plan and implement the plan.

OPE	N: NOT A FINDING:	NOT REVIEWED:	NOT APPLICABLE:
Notes:			